NPS
PRAESTANTIA PER SCIENTIAM

ITACS

Information Technology and Communications Services

Naval Postgraduate School, Monterey, California

201 – Policy for Connecting Non-NPS Owned Computers to the NPS Network (including PDAs)

Approval: ITACS and the IT Task Force

Timeline: Revision date: 1 April 2001; 7 January 2002; 8 June 2004
Effective date: 1 April 2001
Review due: 1 May 2005

Definitions: The NPS network is defined as all electronic data switches, routers, bridges and building data wiring configured to provide electronic and computer data interchange among the members of the network (including data interchanges external to NPS). The ITACS Department is responsible for the design, installation, configuration and operation of the NPS network and associated infrastructure including wireless technologies.

Policy:

1. The network uses wiring closets in most buildings that are OFF LIMITS to all end-users at NPS. Only Network Operations Personnel are permitted to change or configure the equipment and patch-panels in these closets. NO EXCEPTIONS.

2. If you have a non-NPS owned computer you want to connect to the NPS network (desktop, laptop, PDA, etc.), you must register your computer with the Technology Assistance Center in Ingersoll Hall. When a non-NPS owned computer is registered, the person registering it is required to provide the following information:
    - End-user name and NPGS login name (username),
    - The name and phone number of the owner of the computer/PDA,
    - Manufacturer and model of the computer/PDA,
    - Serial number of the computer/PDA,
    - Type of network interface (fixed port, wireless)
    - The MAC address of the NIC card,
    - The name of the machine

   Depending upon which building you want a network connection in you will be issued either a static IP address or directed to use Dynamic Host Configuration Protocol (DHCP). IP addresses or DHCP assignments are specific to each building and often to each floor within a building. Do not use any IP address other than the one you are issued.

3. If you are not certain that you are in compliance with this policy (201), do not make any connections to the NPS network without first consulting with the NPS Network Operations Center in Ingersoll Hall.
4. Not all data ports are active (hot) at NPS. NEVER disconnect the network cable of an NPS computer data port in order to accommodate your non-NPS owned computer.
5. NPS is not responsible for any damage to your personally owned equipment.
6. You are responsible for any damage you may cause to the NPS network environment.
7. NPS will not configure or repair your non-NPS owned computer. NPS system administrators will not add a non-NPS owned computer to the NPGS domain.
8. If you improperly configure your non-NPS owned computer in such a way as to cause the NPS network to be degraded, you will lose your connection privileges.
9. NPS is not responsible for your files, applications or backups on your non-NPS owned computer.
10. All software and applications you utilize MUST be legally owned by or licensed to you, or provided by an NPS owned license.
11. All non-NPS owned computers attached to the NPS network must run approved antivirus software (with current updates) and the operating system must be patched with current hot fixes and service packs AT ALL TIMES.
12. Use of your non-NPS owned computer connected to the NPS network SHALL be subject to all of the rules and Appropriate Use guidelines applicable to ALL computer users at NPS.
13. Use of the NPS dial-up services utilizing personally owned computers is within the scope of this policy (item #2 of this policy does not apply for dialup connections from outside of NPS).
14. Connection to the NPS network via a VPN connection is within the scope of this policy (item #2 of this policy does not apply for VPN connections).